

REMARKS

This responds to the Office Action mailed on January 4, 2006, and the references cited therewith.

Claims 1, 9, and 15 are amended; as a result, claims 1-20 are now pending in this application.

§103 Rejection of the Claims

Claims 1-11, 13, 15, 17-18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Khan et al. (U.S. 6,401,206) in view of Mashayekhi (U.S. 5,818,936) and further in view of Menezes ("Handbook of Applied Cryptography"). It is of course fundamental that in order to sustain an obviousness rejection that each and every step or element in the rejected claims must be taught or suggested in the proposed combination of references. Furthermore, there must exist some motivation to combine the references in the manner being proposed.

The Khan reference is directed to provide a digital identity. The digital identity includes a user name, public information, private information, personal questions and answers supplied, a public-private key pair, a signature, biometric parameters, and personal identifiers. Khan, col. 7, lines 5-12. The digital identity is encrypted by generating a key from select components of the digital identity, such as user name, personal identification number (PIN), and password. Khan, col. 8, lines 30-35. The key may in some cases itself be encrypted using traditional public-private key pairs. Khan, col. 5, lines 43-46.

As has been argued and mentioned, a public key is not a session key. A "session key" is temporary and not permanent and expires automatically upon some even, such as a log out from a service or connection. The Examiner appears to have acknowledged this by citing the Menezes reference for the teaching of a session key; although Applicant notes that the language suggesting that Khan teaches a session key still appears in the Examiner's remarks with respect to the application of Khan vis-à-vis the Applicant's claims. A public key in a private-public key pair is not a session key. To further illustrate this point, the Examiner is invited to view the definitions as understood by those of ordinary skill in the art for "session key" and "public key." See www.whatis.techtarget.com. By definition, a "session key" is frequently changed; this is in

direct opposition to a “public key” that is more permanent and is infrequently changed.

Applicant submits that there is no session key teaching at all in the teachings of Khan and that a public key is not a session key and would not be recognized as such by any one of ordinary skill in the security arts. Thus, Applicant assumes these references were inadvertently carried over by the Examiner from prior actions; especially in view of the fact that the Examiner is now citing Menezes for the teaching of a session key.

In Khan, the digital identity is not intended to be temporary. It is specifically taught and expected to be permanent. The Examiner’s attention is direct to column 8 lines 20-29 where it is stated that the digital identity is generated “only once in its life cycle.” It is acknowledged here that the creation process is time consuming and it is therefore not desired and not desirable for a digital identity to be temporary or non permanent. The importance of this teaching in Khan cannot be understated. The Examiner’s attention is directed to column 11 lines 65 and continuing to column 12 line 32. Here, Khan again emphasizes that the digital identity is intended to be a permanent identity and not a temporary one. Stated another way, the “use” of the digital identity in Khan is permanent and not temporary. Applicant’s amended independent claims make clear that the “use” expires when the “session” expires, and the “session” is associated with the “session key.” Khan requires a permanency that Applicant’s invention teaches away from with the notion of the “session” and “session key.”

In view of this, Applicant respectfully submits that one of ordinary skill in the art would not have been motivated after reading Khan to combine it with Menezes to use session keys because in so doing it would have created a temporary use or usage of digital identities that would frequently expire and require re-encryption and formulation. Such a scenario runs in direct contradiction to the core teachings of permanence in the Khan teaching. Thus, Applicant respectfully submits that one of ordinary skill in the art would not have reasonably included the session keys of Menezes with the teachings of Khan because in so doing the core teachings of Khan would be ignored and violated. Therefore, Applicant asserts that the combination of Khan with Menezes is improper since it is not reasonable to assume any motivation would have existed to combine the two in view of the permanency emphasis in Khan.

Accordingly, Applicant respectfully requests that the rejections be withdrawn and the claims be allowed.

Claims 12, 14, 16 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Khan et al. in view of Mashayekhi and further in view of Menezes as applied to claims 9 and 15 above, and further in view of Spies et al. (U.S. 5,869,565). Claims 12 and 14 are dependent from amended independent claim 9 and claims 16 and 19 are dependent from amended independent claim 15; thus, for the amendments and remarks presented above with respect to claims 9 and 15, the rejections of claims 12, 14, 16, and 19 should be withdrawn and the claims allowed. Applicant respectfully requests an indication of the same.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (513) 942-0224 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

CAMERON MASHAYEKHI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(513) 942-0224

Date

04/04/06

By

Joseph P. Mehrle
Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 4 day of April, 2006.

Peter Rebuffoni

Name

Peter Rebuffoni
Signature